

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 1. (Currently amended) A method for sharing an active secure
2 communication session ~~with a client between a plurality of servers,~~ the method
3 comprising:
4 receiving a first message from ~~the~~ a client at a first server, ~~in the plurality~~
5 of servers, wherein the first message including includes a session identifier that
6 ~~identifies~~ is associated with an active secure communication session ~~with between~~
7 the client and a second server which is different from the first server; ~~and~~
8 retrieving state information using the session identifier, wherein the state
9 information is retrieved by the first server from a database, wherein the state
10 information includes a running message digest, wherein the second server updated
11 the running message digest at the database as messages passed through the active
12 secure communication session between the client and the second server, and
13 wherein the database, the client, the first server, and the second server are
14 different from one another; and
15 using the state information to send a second message from the first server
16 to the client through the active secure communication session.
17 ~~if the session identifier does not correspond to an active secure~~
18 ~~communication session on the first server, establishing an active secure~~
19 ~~communication session with the client on the first server by,~~
20 attempting to retrieve state information associated with the
21 ~~session identifier for an active secure communication session~~

22 ~~between the client and a second server, wherein the state~~
23 ~~information is retrieved from a third server which is different from~~
24 ~~the client, wherein the state information includes a session~~
25 ~~encryption key associated with the active secure communication~~
26 ~~session between the client and the second server, wherein the first~~
27 ~~server is different from the second server,~~

28 ~~if the state information for the active secure communication~~
29 ~~session is retrieved, using the state information including the~~
30 ~~encryption keys to share the active secure communication session~~
31 ~~established between the client and the second server for subsequent~~
32 ~~communications between the client and the first server without~~
33 ~~having to set up a new secure communication session between the~~
34 ~~client and the first server, wherein the state information is purged~~
35 ~~from the second server after the state information is retrieved by~~
36 ~~the first server, and~~

37 ~~if the state information for the active secure communication~~
38 ~~session is not retrieved, communicating with the client to establish~~
39 ~~the active secure communication session with the client.~~

1 2-8. (Canceled).

1 9. (Original) The method of claim 1, further comprising initially
2 establishing an active secure communication session between the client and the
3 second server, the active secure communication session being identified by the
4 session identifier.

1 10. (Currently amended) The method of claim 1, wherein ~~attempting to~~
2 ~~retrieving~~ the state information includes authenticating and authorizing the first
3 server.

1 11-12 (Canceled).

1 13. (Currently amended) A computer-readable storage medium storing
2 instructions that when executed by a computer cause the computer to perform a
3 method for sharing an active secure communication session ~~with a client between~~
4 ~~a plurality of servers, the method~~ comprising:

5 receiving a first message from ~~the a~~ client at a first server, ~~in the plurality~~
6 ~~of servers, wherein~~ the first message ~~including~~ includes a session identifier that
7 ~~identifies~~ is associated with an active secure communication session ~~with between~~
8 the client and a second server which is different from the first server; and

9 retrieving state information using the session identifier, wherein the state
10 information is retrieved by the first server from a database, wherein the state
11 information includes a running message digest, wherein the second server updated
12 the running message digest at the database as messages passed through the active
13 secure communication session between the client and the second server, and
14 wherein the database, the client, the first server, and the second serve are different
15 from one another; and

16 using the state information to send a second message from the first server
17 to the client through the active secure communication session.

18 ~~if the session identifier does not correspond to an active secure~~
19 ~~communication session on the first server, establishing an active secure~~
20 ~~communication session with the client on the first server by,~~

21 ~~attempting to retrieve state information associated with the~~
22 ~~session identifier for an active secure communication session~~

~~between the client and a second server, wherein the state
information is retrieved from a third server which is different from
the client, wherein the state information includes a session
encryption key associated with the active secure communication
session between the client and the second server, wherein the first
server is different from the second server,~~

~~if the state information for the active secure communication
session is retrieved, using the state information including the
encryption keys to share the active secure communication session
established between the client and the second server for subsequent
communications between the client and the first server without
having to set up a new secure communication session between the
client and the first server, wherein the state information is purged
from the second server after the state information is retrieved by
the first server, and~~

~~if the state information for the active secure communication
session is not retrieved, communicating with the client to establish
the active secure communication session with the client.~~

14-20. (Canceled).

21. (Original) The computer-readable storage medium of claim 13,
wherein the method further comprises initially establishing an active secure
communication session between the client and the second server, the active secure
communication session being identified by the session identifier.

1 22. (Currently amended) The computer-readable storage medium of claim
2 | 13, wherein ~~attempting to retrieve~~ing the state information includes authenticating
3 and authorizing the first server.

1 23-24 (Canceled).

1 25. (Currently amended) An apparatus that shares a secure communication
2 session with a client between a plurality of servers, comprising:

3 a receiving mechanism configured to receive a first message from a client
4 at a first server, wherein the first message includes a session identifier that is
5 associated with an active secure communication session between the client and a
6 second server which is different from the first server;~~at a first server in the~~
7 ~~plurality of servers, that receives a message from the client, the message including~~
8 ~~a session identifier that identifies a secure communication session with the client;~~

9 a retrieving mechanism configured to retrieve state information using the
10 session identifier, wherein the state information is retrieved by the first server
11 from a database, wherein the state information includes a running message digest,
12 wherein the second server updated the running message digest at the database as
13 messages passed through the active secure communication session between the
14 client and the second server, and wherein the database, the client, the first server,
15 and the second server are different from one another; and

16 a sending mechanism configured to use the state information to send a
17 second message from the first server to the client through the active secure
18 communication session.

19 ~~an examination mechanism that examines the session identifier; and~~
20 ~~a session initialization mechanism, on the first server, wherein if the~~
21 ~~session identifier does not correspond to an active secure communication session~~

22 on the first server, the session initialization mechanism is configured to establish
23 an active secure communication session with the client by,
24 attempting to retrieve state information associated with the
25 session identifier for an active secure communication session
26 between the client and a second server, wherein the state
27 information is retrieved from a third server which is different from
28 the client, wherein the state information includes a session
29 encryption key associated with the active secure communication
30 session between the client and the second server, wherein the first
31 server is different from the second server,
32 if the state information for the active secure communication
33 session is retrieved, using the state information including the
34 encryption keys to share the active secure communication session
35 established between the client and the second server for subsequent
36 communications between the client and the first server without
37 having to set up a new secure communication session between the
38 client and the first server, and
39 if the state information for the active secure communication
40 session is not retrieved, communicating with the client to establish
41 the active secure communication session with the client.

1 26-32. (Canceled)

1 33. (Currently amended) The apparatus of claim 25, wherein the session
2 ~~initialization~~retrieving mechanism is configured to authenticate and authorize the
3 first server prior to ~~receiving~~retrieving the state information.

1 34-35 (Canceled).